

1 BILAL A. ESSAYLI  
United States Attorney  
2 CHRISTINA T. SHAY  
Assistant United States Attorney  
3 Chief, Criminal Division  
JONATHAN GALATZAN  
4 Assistant United States Attorney  
Chief, Asset Forfeiture & Recovery Section  
5 JAMES E. DOCHTERMAN (Cal. Bar No. 256396)  
Assistant United States Attorney  
6 Asset Forfeiture & Recovery Section  
312 North Spring Street, 11th Floor  
7 Los Angeles, California 90012  
Telephone: (213) 894-2686  
8 Facsimile: (213) 894-6269  
E-mail: James.Dochterman@usdoj.gov  
9

Attorneys for Plaintiff  
10 UNITED STATES OF AMERICA

11 UNITED STATES DISTRICT COURT  
12  
13 FOR THE CENTRAL DISTRICT OF CALIFORNIA  
14 WESTERN DIVISION

15 UNITED STATES OF AMERICA,  
16 Plaintiff,  
17 v.  
18 VIRTUAL CURRENCY AND  
\$2,061,517.68 IN U.S. CURRENCY,  
19 Defendants.  
20  
21  
22  
23

Case No. 2:25-CV-04631

**COMPLAINT FOR FORFEITURE**

18 U.S.C. § 981(a)(1)(A) and (C)  
[FBI]

24 Plaintiff United States of America brings this claim against  
25 defendants Virtual Currency and \$2,061,517.68 in U.S. Currency, and  
26 alleges as follows:  
27  
28

**JURISDICTION AND VENUE**

1. Plaintiff United States of America brings this in rem forfeiture action pursuant to 18 U.S.C. § 981(a)(1)(A) and (C).<sup>1</sup>

2. This Court has jurisdiction over the matter under 28 U.S.C. §§ 1345 and 1355.

3. Venue lies in this District pursuant to 28 U.S.C. §§ 1355 and 1395.

**PERSONS AND ENTITIES**

4. The plaintiff is the United States of America.

5. The defendants Virtual Currency (the "defendant Virtual Currency") and \$2,061,517.68 in U.S. Currency (the "defendant currency") are collectively referred to herein as "the defendant assets." The defendant Virtual Currency<sup>2</sup> consists of the following:

a. The USDT<sup>3</sup> transferred to the government following the issuance of a July 29, 2024 federal seizure warrant, consisting of an equivalent amount of USDT frozen by the government on August 25, 2023, associated with the virtual currency addresses listed below (collectively, the "USDT Addresses") and more specifically described as (i) 1,867,051.090192 USDT associated with virtual currency addresses ending in "d774", "43ac", and "2cfd" on the Ethereum

---

<sup>1</sup> All dates set forth in the Complaint are on or about the dates indicated, and all amounts or sums are approximate.

<sup>2</sup> Virtual currencies are digital tokens of value circulated as substitutes for traditional fiat currency and sent to and received from virtual currency addresses. Virtual currencies are not issued by any government or bank like traditional fiat currency, such as the U.S. dollar, but rather are generated and controlled through computer software.

<sup>3</sup> USDT is also known as Tether and is a "stablecoin" type of virtual currency whose value is pegged to the U.S. dollar.

1 network; and (ii) 131,864.958226 USDT associated with virtual  
2 currency addresses ending in "diwg" and "Qnql" on the Tron network;

3           b. The virtual currency seized following the issuance of  
4 a federal seizure warrant on August 25, 2023 from virtual currency  
5 wallets (the "August 2023 Wallets"), which are more particularly  
6 described as (i) 0.98764847 BTC, 0.748382350077596 ETH, 2,225.664765  
7 TRX, 27,440.236603 USDT on the Ethereum network and 12,786.27805 USDT  
8 on the Tron network; (ii) 0.0356658763729553 ETH, 1,000 USDT on the  
9 Ethereum network, and 88.306384186 TON on the Ethereum network; (iii)  
10 0.116887384939969 ETH, and 50 USDT on the Ethereum network; (iv)  
11 0.00008155 BTC; (v) 80,248.604484476 TON on the Ethereum network;  
12 (vi) 63,776.869432785 EVER; (vii) 0.00154878 ETH; (viii) 162.86215848  
13 BTC; (ix) 1.44223059 BTC; (x) 78.74 XMR; (xi) 47.81 XMR; (xii)  
14 1.84681961 XMR; (xiii) 0.0235862 XMR; (xiv) 125.0562078 XMR; (xv)  
15 0.04399859 XMR; (xvi) 0.1599822 BTC; and (xvii) 5.31848493 BTC; and

16           c. The virtual currency seized following the issuance of  
17 a federal seizure warrant on April 18, 2025 from virtual currency  
18 wallets (the "April 2025 Wallets"), which are more particularly  
19 described as (i) 22,622.300445 TRX, and 718,191.493006 USDT on the  
20 Tron network; (ii) 30.86066699 BTC; and (iii) 0.015326022542196328  
21 ETH, and 262.30293 USDT on the Ethereum network.

22           6. The defendant currency represents the U.S. dollar  
23 equivalent to the USD Coin ("USDC")<sup>4</sup> frozen by the government,  
24 associated with the virtual currency addresses listed below  
25 (collectively, the "USDC Addresses"), transferred to the government  
26 on October 27, 2023 following the issuance of a federal seizure  
27

---

28           <sup>4</sup> USDC is a "stablecoin" type of virtual currency whose value is  
pegged to the U.S. dollar.

1 warrant for the contents of the USDC Addresses, and is more  
2 particularly described as (i) 839,993.06 USDC associated with a  
3 virtual currency address ending in "d774" on the Ethereum network  
4 (ii) 74,248.29 USDC associated with a virtual currency address ending  
5 in "TEPd" on the Tron network; (iii) 49,914.71 USDC associated with a  
6 virtual currency address ending in "43ac" on the Ethereum network;  
7 and (iv) 1,097,361.62 USDC associated with a virtual currency address  
8 ending in "2cfd" on the Ethereum network.

9 7. The defendant assets were seized by the Federal Bureau of  
10 Investigation at 11000 Wilshire Boulevard, Suite 1700 in Los Angeles,  
11 California and are currently in or will be transferred to the custody  
12 of the United States Marshals Service in this District, where they  
13 will remain subject to this Court's jurisdiction during the pendency  
14 of this action.

15 8. The interests of Rustam Rafailevich Gallyamov and the  
16 victims of the Qakbot conspiracy may be adversely affected by these  
17 proceedings.

#### 18 BASIS FOR FORFEITURE

#### 19 I. Gallyamov is Indicted as A Result of His Orchestration of a 20 Scheme to Infect Victim Computers and Extort Ransom Payments 21 from Victims.

22 9. Qakbot (or Qbot) was a malicious computer software  
23 developed, deployed, and controlled since 2008 by members of a  
24 cybercriminal conspiracy led by Gallyamov. From at least 2019,  
25 Qakbot conspirators infected hundreds of thousands of victim  
26 computers in the Central District of California and elsewhere with  
27  
28

1 the Qakbot malware,<sup>5</sup> thereby gaining unauthorized access to and  
2 control of those computers. This network of compromised victim  
3 computers was commonly referred to as the Qakbot botnet.<sup>6</sup>

4 10. After the Qakbot botnet was disrupted in an international  
5 law enforcement action in August 2023, the Qakbot conspirators  
6 continued to seek and gain unauthorized access to victim computers  
7 using means other than the Qakbot botnet. One technique that they  
8 used was conducting spam bomb attacks<sup>7</sup> on employees of victim  
9 companies and then posing as information technology workers to trick  
10 victims into executing malicious code or otherwise providing access  
11 to company computers.

12 11. Qakbot conspirators used their unauthorized access to  
13 victim computers to facilitate the further infection of those victim  
14 computers with additional malicious software in the form of  
15 ransomware. In coordination with the Qakbot conspiracy, ransomware  
16 actors, including Prolock, Doppelpaymer, Egregor, REvil, Conti, Name  
17 Locker, Black Basta and Cactus, infiltrated victim computer networks  
18 and deployed ransomware. Typically, as part of these ransomware  
19 attacks, data was also stolen from victim computers. Victims were  
20 then extorted to regain access to their data and to prevent the  
21 further dissemination of their private data by the attackers.

---

24 <sup>5</sup> "Malware" is malicious computer software intended to cause a  
25 victim computer to behave in a manner inconsistent with the, and  
typically unbeknownst by, the victim computer's owner or user.

26 <sup>6</sup> A "botnet" is a network of infected computers (each a "bot")  
27 that have been infected with malware and are being controlled by a  
group.

28 <sup>7</sup> A "spam bomb attack" is a type of cyberattack that floods a  
victim's inbox by using automated techniques to sign the victim up  
for a large number of email subscriptions.

1           12. Ransomware victims typically paid ransoms in Bitcoin (BTC).  
2 Gallyamov and the Qakbot conspirators were paid a share of the ransom  
3 for each victim whose computers were compromised by the Qakbot  
4 conspiracy.

5           13. On May 2, 2025, in case No. 2:25-CR-340-SB, a grand jury in  
6 the Central District of California returned an indictment charging  
7 Gallyamov with violations of 18 U.S.C. §§ 371 (conspiracy to violate  
8 18 U.S.C. § 1030) and 1349 (conspiracy to violate 18 U.S.C. § 1343)  
9 for his role in the Qakbot conspiracy. The indictment also includes  
10 a forfeiture allegation providing that upon his conviction, Gallyamov  
11 must forfeit all traceable proceeds, such as the defendant assets, of  
12 the Qakbot conspiracy.

13           14. As discussed below, the defendant assets are subject to  
14 forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and (C) because they  
15 constitute traceable proceeds of and were involved in money  
16 laundering offenses pertaining to the payment of ransoms for  
17 computers infected by ransomware as a result of computer intrusions  
18 by members of the Qakbot conspiracy.

19           15. The virtual currencies discussed in this complaint include:

20           a. BTC, a virtual currency that exists on the Bitcoin  
21 blockchain.<sup>8</sup>

22           b. Ether ("ETH"), a virtual currency that exists on the  
23 Ethereum blockchain (also referred to as the Ethereum network).  
24

---

25           <sup>8</sup> Many virtual currencies publicly record all of their virtual  
26 currency transactions (as well as each virtual currency address  
27 balance) on what is known as a "blockchain." The blockchain is  
28 essentially a public ledger, run by a decentralized network of  
computers and containing an immutable and historical record of every  
transaction utilizing that blockchain's technology. There are  
different blockchains for different types of virtual currencies.

1 c. The stablecoin USDT ("Tether"), which exists on  
2 multiple blockchains, including the Ethereum and Tron blockchains.

3 d. The stablecoin USDC, which exists on multiple  
4 blockchains, including the Ethereum and Tron blockchains.

5 e. Tron ("TRX"), a virtual currency that exists on the  
6 Tron blockchain (also referred to as the Tron network).

7 f. Toncoin ("TON"), a virtual currency that operates on  
8 the Ethereum blockchain; and

9 g. Monero ("XMR"), a privacy-enhanced virtual currency  
10 that operates on the Monero blockchain.

11 **II. The Defendant Assets Constitute Traceable Ransom and Laundered**  
12 **Proceeds.**

13 16. As part of the ransom and money laundering scheme, upon  
14 receipt of the initial ransom proceeds, Qakbot conspirators engaged  
15 in multiple transactions moving virtual currency through a series of  
16 intermediary addresses in a manner common to money laundering schemes  
17 and intended to conceal the criminal origin of the proceeds. These  
18 transactions involved unnecessary or duplicative transactions into  
19 and out of wallets or addresses and through decentralized services on  
20 the blockchain to frustrate tracing and avoid attention from law  
21 enforcement. As described below, ransom proceeds were also comingled  
22 with other victims' ransom proceeds as well as unknown sources,  
23 further demonstrating the coconspirators intent to conceal the  
24 criminal origin of the virtual currency.

25 **A. The August 2023 Wallets Held Ransom and Laundered**  
26 **Proceeds.**

27 17. Based on their review of blockchain transaction records,  
28 records from virtual assets service providers, Qakbot conspirator  
communications and records, and analysis using commercial blockchain

1 analysis tools, law enforcement officers determined that numerous  
2 deposits made to the August 2023 Wallets consisted of ransoms paid to  
3 ransomware groups, which in turn paid Gallyamov.

4 18. The deposits of ransoms to the August 2023 wallets  
5 primarily came from clusters of addresses identified by law  
6 enforcement as belonging to ransomware groups or known ransomware  
7 actors. Analysis by law enforcement showed that ransoms paid by  
8 victims were often collected or pooled in clusters of addresses  
9 associated with that ransomware group before shares of the ransom  
10 payment were parceled out, including to Gallyamov. Analysis by law  
11 enforcement further showed that at times virtual currency held in the  
12 August 2023 Wallets was converted from BTC to other forms of virtual  
13 currency using blockchain-based services or virtual asset service  
14 providers.

15 19. Analysis of transactions involving the August 2023 Wallets  
16 between September 2022 and April 2023 showed that ransom payments  
17 made to Gallyamov in BTC made up more than 80 percent of the value of  
18 the virtual currency seized from the August 2023 Wallets.

19 20. The ransom payments to the August 2023 Wallets include but  
20 are not limited to the following:

21 a. On October 13, 2022, a New York law firm paid a ransom  
22 of 15.61359 BTC to a ransomware group. That payment moved through a  
23 series of intermediary addresses associated with a known Qakbot  
24 coconspirator ("Coconspirator 1"). That same day, 1.561359 BTC,  
25 identified by Coconspirator 1 to Gallyamov as a 10% payment for the  
26 New York law firm ransom was paid into an address in the August 2023  
27 Wallets. The source of the funds for that payment was a comingled  
28



1 39.999865 BTC ransom paid by a Wisconsin marketing company to another  
2 Qakbot-affiliated ransomware group on May 12, 2022.

3 b. On November 16, 2022, an Indiana technology company  
4 was the victim of a ransomware attack and paid a ransom. On November  
5 28, 2022, a deposit of 15.006 BTC was made from the cluster of  
6 addresses associated with Coconspirator 1 to an address in the August  
7 2023 Wallets. Gallyamov identified that payment to a coconspirator  
8 as his share of the ransom paid by the Indiana technology company.

9 c. On December 16, 2022, a Missouri media company paid a  
10 ransom of 58.4521985 BTC to a ransomware group. After moving through  
11 a series of intermediary addresses, 19.1543 BTC of the ransom was  
12 paid to an address in the August 2023 Wallets. Gallyamov recorded  
13 that December 20, 2022, payment in his payment ledger, and identified  
14 it to a coconspirator as his share of the comingled ransom paid by a  
15 Tennessee music company in connection with a ransomware attack.

16 d. In March 2023, a Colorado technology company paid a  
17 ransom of 179.760005 BTC to a ransomware group. Gallyamov recorded a  
18 March 20, 2023, payment of 17.976 BTC, which was paid to an address  
19 in the August 2023 wallets, in his payment ledger as his share of the  
20 ransom paid by the Colorado technology company.

21 e. In September 2022, a Maryland bank was the victim of a  
22 ransomware attack and paid a ransom of approximately \$175,000 in BTC.  
23 On October 19, 2022, 0.8935 BTC, identified by Coconspirator 1 to  
24 Gallyamov as a 10% payment for the Maryland bank ransom was paid into  
25 an address in the August 2023 Wallets.

26 f. On November 14, 2022, 8.631 BTC was paid into an  
27 address in the August 2023 Wallets from the cluster of addresses  
28 associated with Coconspirator 1. Gallyamov recorded that payment in

1 his payment ledger as his share of the ransom paid by an Austrian  
2 hospitality company.

3 g. On November 14, 2022, 5.5335 BTC was paid into an  
4 address in the August 2023 Wallets from the cluster of addresses  
5 associated with Coconspirator 1. Gallyamov recorded that payment in  
6 his payment ledger as his share of the ransom paid by an Illinois  
7 engineering firm.

8 h. On September 26, 2022, 1.0315 BTC was paid into an  
9 address in the August 2023 Wallets from the cluster of addresses  
10 associated with Coconspirator 1. Gallyamov identified that payment  
11 to a coconspirator as his share of the ransom paid by a Canadian home  
12 furnishing company. The source of the funds for that payment of  
13 1.0315 BTC was a 5.14250156 BTC ransom paid by a Kentucky law firm to  
14 a ransomware group.

15 i. On March 13, 2023, 4.9209 BTC was paid into an address  
16 in the August 2023 Wallets. Gallyamov identified that payment in his  
17 payment ledger as his share of the ransom paid by a Virginia maritime  
18 engineering company. The source of the funds for that payment of  
19 4.9209 BTC, in turn, was a 243.9422269 BTC ransom paid by a North  
20 Dakota legal outsourcing company.

21 j. On March 7, 2023, a New York law firm paid a ransom of  
22 40.204054 BTC to a ransomware group. On March 13, 2023, 4.0204 BTC  
23 originating from that ransom payment was deposited into an address in  
24 the August 2023 Wallets. Gallyamov identified that payment in his  
25 payment ledger as his share of the ransom paid by the New York law  
26 firm.

27 k. On November 30, 2022, an Alabama bank paid a ransom of  
28 11.595551815 BTC to a ransomware group. On December 29, 2022,

1 1.1599433 BTC originating from that ransom payment was deposited into  
2 an address in the August 2023 Wallets. Gallyamov identified that  
3 payment in his payment ledger as his share of the ransom paid by the  
4 Alabama bank.

5 1. On March 13, 2023, a Michigan manufacturing company  
6 paid a ransom of 4.08106996 BTC to a ransomware group. On March 16,  
7 1.9895 BTC from that ransom payment was deposited into an address in  
8 the August 2023 Wallets. Gallyamov identified that payment in his  
9 payment ledger as his share of the ransom paid by a North Carolina  
10 freight company. Then, on April 13, 2023, an additional 1.6683 BTC  
11 originating from the ransom payment was deposited into another  
12 address in the August 2023 Wallets. Gallyamov identified that  
13 payment in his payment ledger as his share of the ransom paid by a  
14 New York food company.

15 m. On September 29, 2022, 63.14 BTC was deposited into an  
16 address in the August 2023 Wallets. This payment originated from a  
17 cluster of addresses associated with a Qakbot-affiliated ransomware  
18 group. The address that sent the 63.14 BTC had received a total of  
19 143.50 BTC in an earlier transaction and sent 40.459948 BTC to a  
20 cluster of addresses associated with Coconspirator 1. Gallyamov  
21 provided the address that received 63.14 BTC to Coconspirator 1, who  
22 sent Gallyamov the following calculation, indicating that the 63.14  
23 BTC represented Gallyamov's share of ransom proceeds: "143.5 - 12% =  
24 128.26 / 2 = 63,14."

25 **B. The USDC Addresses and USDT Addresses Held Ransom and**  
26 **Launched Proceeds that Were Used to Promote the Qakbot**  
**Conspiracy.**

27 21. In the same file where law enforcement identified  
28 information about the August 2023 Wallets, investigators also found

1 details identifying the USDC Addresses and the USDT Addresses. Those  
2 addresses corresponded to virtual currency stored on ledger hardware  
3 wallets owned by Gallyamov.

4 22. The wallet addresses stored in those ledger devices were on  
5 the Ethereum and Tron blockchains, which are capable of holding  
6 multiple types of virtual currency or tokens at a single wallet  
7 address. The four USDC Addresses are the same addresses as four of  
8 the six USDT Addresses, with both USDC and USDT seized from the same  
9 ledger addresses. The majority of the virtual assets held in the  
10 USDT Addresses and the USDC Address were held on the four overlapping  
11 wallet addresses.

12 23. Launderers often convert laundered virtual currency to  
13 stablecoins and transfer those proceeds into pooling addresses and  
14 thereafter use the laundered funds to pay expenses or coconspirators.  
15 These transfers are made to conceal the underlying source of the  
16 funds and to avoid alerting law enforcement to the criminal activity  
17 connected to the laundered funds. By moving crime proceeds through  
18 numerous addresses before parking them in pooling accounts like the  
19 USDT Addresses and USDC Addresses, Gallyamov attempted to conceal the  
20 nature, source, location, ownership, or control of the proceeds.

21 24. Based on their review of blockchain transaction records,  
22 records from virtual assets service providers, Qakbot conspirator  
23 communications and records, and analysis using commercial blockchain  
24 analysis tools, law enforcement officers identified the funding  
25 sources for the USDT Addresses and USDC Addresses. They were funded,  
26 primarily with USDC and USDT originating from virtual currency  
27 exchanges outside the United States in 2021 and 2022.

1           25. Analysis of transactions involving the USDT Addresses and  
2 USDC Addresses show that they were used in money laundering  
3 transactions and were also used to make payments of ransom proceeds  
4 to Qakbot coconspirators to facilitate the operation of the  
5 conspiracy. Those transactions include but are not limited to the  
6 following:

7           a. On August 2, 2022, receiving 1,381 USDT from a  
8 coconspirator.

9           b. On April 17, 2023, sending 50,000 USDT to an address  
10 in the August 2023 Wallets, comingling the ransom proceeds.

11           c. On July 3, 2023, sending 130,000 USDT in two  
12 transactions to an address in the August 2023 Wallets, comingling the  
13 ransom proceeds.

14           d. On August 19, 2023, sending 10,000 USDT to an address  
15 in the August 2023 Wallets, comingling the ransom proceeds.

16           e. On February 1, 2022, sending 200,000 USDT to an  
17 address provided by an individual who would exchange the USDT for  
18 fiat currency for a fee.

19           f. On February 24, 2023, sending 300,000 USDT to an  
20 address provided by an individual who would exchange the USDT for  
21 fiat currency for a fee.

22           g. On July 25, 2023, sending 133,900 USDT to an address  
23 provided by an individual who would exchange the USDT for fiat  
24 currency for a fee.

25           26. Sending payments to addresses identified by Qakbot  
26 coconspirators for payment, including the following:

27           a. On April 3, 2022, sending 1,800 USDT to a  
28 coconspirator.

1           b.    On July 4, 2022, sending 1,800 USDT to a  
2 coconspirator.

3           c.    On July 8, 2022, sending 750 USDT to a coconspirator.

4           d.    On July 15, 2022, sending 20,400 USDT to one  
5 coconspirator, and 15,000 USDT to a second coconspirator.

6           e.    On September 2, 2022, sending 1,800 USDT to a  
7 coconspirator.

8           f.    On December 29, 2022, sending 3,000 USDT to one  
9 coconspirator, 3,600 USDT to a second coconspirator, and 6,400 USDT  
10 to a third coconspirator.

11          g.    On December 30, 2022, sending 15,000 USDT to each of  
12 three coconspirators.

13          h.    On April 3, 2023, sending 1,500 USDT to one  
14 coconspirator and 3,250 USDT to a second coconspirator.

15          i.    On June 30, 2023, sending 21,400 USDT to a  
16 coconspirator.

17           **C.    The April 2025 Wallets Received Ransom and Laundered**  
18           **Proceeds.**

19           27.   Based on their review of blockchain transaction records,  
20 records from virtual assets service providers, Qakbot conspirator  
21 communications and records, and analysis using commercial blockchain  
22 analysis tools, law enforcement officers determined that numerous  
23 deposits made to the April 2025 Wallets consisted of ransoms paid to  
24 ransomware groups, which in turn paid Gallyamov. Those ransom  
25 payments to the August 2023 Wallets include but are not limited to  
26 the following:

27           a.    In December 2024, a New Jersey company was the victim  
28 of a ransomware attack and paid a ransom of 15.94 BTC on December 23,

1 2024. That payment was immediately split up, with 12.754 BTC going  
2 to an address in the April 2025 Wallets. The funds were thereafter  
3 dissipated from the that wallet address in a series of transfers of  
4 roughly \$40,000 to \$50,000 in BTC to virtual asset service providers  
5 outside the United States.

6 b. In January 2025, a Wisconsin Company was the victim of  
7 a ransomware attack and paid a ransom of 20.274 BTC on January 16,  
8 2025. That payment was immediately split up, with 14.189 BTC going  
9 to an address in the April 2025 Wallets. The funds were thereafter  
10 dissipated from the that wallet address in a series of transfers to  
11 non-custodial instant cryptocurrency exchanges.

12 c. In January 2025, a Pennsylvania company was the victim  
13 of a ransomware attack and paid a ransom of 28.31 BTC on January 17,  
14 2025. That payment was immediately split up, with 19.8142 BTC going  
15 to an address in the April 2025 Wallets.

16 d. In January 2025, a Maryland company was the victim of  
17 a ransomware attack and paid a ransom of 9.417 BTC on January 24,  
18 2025, to an address in the April 2025 Wallets.

**FIRST CLAIM FOR RELIEF**

28. Paragraphs 1 through 27 are incorporated by reference as if fully set forth herein.

29. Based on the above, plaintiff alleges that the defendant assets constitute property involved in multiple or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), (a)(1)(B)(i), (a)(2)(A), (a)(2)(b)(i) and/or (h), or property traceable to such property, with the specified unlawful activity being a violation of 18 U.S.C. §§ 1030 (relating to computer fraud and abuse) and/or 1343 (wire fraud). The defendant assets are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

**SECOND CLAIM FOR RELIEF**

30. Paragraphs 1 through 27 are incorporated by reference as if fully set forth herein.

31. Based on the above, plaintiff alleges that the defendant assets constitute property involved in multiple or attempted transactions in violation of 18 U.S.C. § 1957(a), with the specified unlawful activity being a violation of 18 U.S.C. §§ 1030 (relating to computer fraud and abuse) and/or 1343 (wire fraud). The defendant assets are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

**THIRD CLAIM FOR RELIEF**

32. Paragraphs 1 through 27 are incorporated by reference as if fully set forth herein.

33. Based on the above, plaintiff alleges that the defendant assets constitute or are derived from proceeds traceable to, or a conspiracy to commit violations of 18 U.S.C. §§ 1030 (relating to computer fraud and abuse), which is a specified unlawful activity as



defined in 18 U.S.C. § 1956(c)(7)(D), and/or 1343 (wire fraud), which is a specified unlawful activity as defined in 18 U.S.C. §§ 1956(c)(7)(A) and 1961(1)(B). The defendant assets are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff the United States of America prays:

(a) that due process issue to enforce the forfeiture of the defendant assets;

(b) that due notice be given to all interested parties to appear and show cause why forfeiture should not be decreed;

(c) that this Court decree forfeiture of the defendant assets to the United States of America for disposition according to law; and

(d) for such other and further relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Dated: May 22, 2025

BILAL A. ESSAYLI  
United States Attorney  
CHRISTINA T. SHAY  
Assistant United States Attorney  
Chief, Criminal Division  
JONATHAN GALATZAN  
Assistant United States Attorney  
Chief, Asset Forfeiture & Recovery  
Section

/s/ James E. Dochterman  
JAMES E. DOCHTERMAN  
Assistant United States Attorney  
Asset Forfeiture & Recovery Section

Attorneys for Plaintiff  
UNITED STATES OF AMERICA

**VERIFICATION**

I, Jacob T. Frederick, hereby declare that:

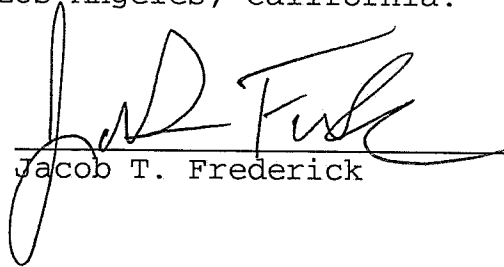
1. I am a Special Agent with the Federal Bureau of Investigation.

2. I have read the above Complaint for Forfeiture and know the contents thereof.

3. The information contained in the Complaint is either known to me personally, was furnished to be my official government sources, or was obtained pursuant to legal process. I am informed and believe that the allegations set out in the Complaint are true.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on May 22, 2025, at Los Angeles, California.



Jacob T. Frederick